

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF
APPLE iPHONE, CURRENTLY LOCATED
AT HSI PORTLAND, ME, 1 CITY
CENTER, 4TH FLOOR, PORTLAND, ME
04103

Case No. 2:24-mj-229-KFW

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, David Fife, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent (SA) with Homeland Security Investigations (HSI) and have been since August 2009. I am currently assigned to HSI's Portland, Maine office. I have participated in numerous criminal investigations, to include those involving financial fraud, wire fraud, money laundering, and computer fraud/intrusions. In my career, I have used various investigative tools and techniques, including the use of search warrants. This includes search warrants for cellular phones.

3. This affidavit is intended to show that there is probable cause for the requested search warrant. The facts set forth in this affidavit are based upon my personal knowledge, information obtained during my participation in this investigation,

including information provided by other investigators, my review of documents and computer records related to this investigation, and information gained through my training and experience.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a blue iPhone 13, model A2482, bearing IMEI 351138107309877, hereinafter the “Device.” The Device is currently located at the HSI Portland, ME evidence room, 1 City Center, 4th Floor, Portland, ME 04103.



5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On June 10, 2024, Andre Hill was charged by criminal complaint with six counts of bank fraud, in violation of 18 U.S.C. § 1344. The complaint was supported by my affidavit and sworn before United States Magistrate Judge Karen Frink Wolf. An arrest warrant was issued to arrest Andre Hill. A copy of my affidavit in support of the criminal complaint is attached as Exhibit 1 and incorporated here.

7. On July 1, 2024, a state trooper with the Massachusetts State Police pulled over a BMW with Massachusetts plate 3PKM68 for speeding. Andre Hill, identified by his Florida driver's license, was the driver. Notably, this is the same vehicle referenced in the criminal complaint affidavit. (Exhibit 1). Based on the arrest warrant issued pursuant to the criminal complaint filed in this Court, the trooper took Hill into custody. The vehicle was impounded and inventoried. Inside the vehicle were four prepaid Vanilla brand VISA gift cards and one SecureSpend prepaid VISA gift card, which are pictured below.



8. Based on my training and experience, prepaid gift cards, including Vanilla and SecureSpend gift cards, are commonly used in criminal schemes to store, transfer, and/or conceal fraud proceeds. Vanilla's VISA gift cards can also be loaded onto digital wallets such as Apple Pay, Samsung Pay, and Google Pay (SecureSpend cards, however, cannot generally be added to digital wallets). *See* <https://www.vanillagift.com/catalog>. As explained in the criminal complaint affidavit (Exhibit 1), Hill's scheme involved the use of digital wallets.

9. On July 2, 2024, Hill came into federal custody. He was arrested by HSI agents. Pursuant to the arrest, the agents detained the Device, which Hill had with him in his personal effects transferred to HSI by the Massachusetts State Police.

10. As set forth more fully in the criminal complaint affidavit (Exhibit 1), Hill participated in a scheme to load stolen Bangor Savings Bank (BSB) accounts into digital

wallets, including Apple Pay, that he then used to make purchases in Maine without the victim account holders' knowledge or consent. Because all of the transactions were made using one or more digital wallets, Hill used his smartphone to complete the transactions. Indeed, as explained in the criminal complaint affidavit (Exhibit 1), Hill can be seen on security footage manipulating his cell phone and using it to make purchases and get cash back at Hannaford self-check out machines.

11. Based on evidence provided by BSB, stolen BSB debit card numbers were loaded onto at least two types of digital wallets for fraudulent purchases in Maine: Apple Pay and Samsung Pay. Apple Pay allows users of Apple products, such as iPhones, to add credit, debit, or prepaid cards to the Wallet app on their devices and then use the device to make contactless purchases in lieu of using a physical card. See <https://www.apple.com/apple-pay/>.

12. As an example of how Apple Pay was used in the scheme, according to bank records from BSB, on January 9, 2023, three transactions were made at a Hannaford in Portland between 1:25 and 1:27 PM using a stolen BSB debit card ending in 1761. Surveillance video from self-checkout kiosks at the store shows Hill using a phone to make the transactions. BSB records also show that, at 1:19 PM, there was a \$0 transaction on Apple Pay using the stolen BSB card ending in 1761. This implies that, at 1:19, Hill loaded the debit card ending in 1761 into Apple Pay and, minutes later, used Apple Pay on an iPhone to make purchases and withdraw funds at the Hannaford.

13. BSB records show that other stolen debit card numbers identified in the complaint affidavit (Exhibit 1)—e.g. debit cards ending in 1443, 8488, and 7888—transacted with Apple Pay on January 9, 2023 before being used to make purchases in

Maine on that date. This suggests that Hill used Apple Pay, and an iPhone, to engage in the fraud.

14. The Device detained from Hill is an Apple iPhone 13, and, as evidenced by the photo, has a significantly damaged screen and appears quite worn. The iPhone 13 was officially released in September of 2021, and is two models removed from the current iPhone (the iPhone 15). Consequently, it is likely that the Device is one that Hill has owned for several years, and could therefore be the same device he possessed and/or used during the fraudulent activity in January and February of 2023, described in criminal complaint affidavit (Exhibit 1).

15. Additionally, Apple advertises to iPhone users who use Apple Pay that, “[i]f you upgrade to a new iPhone, you can automatically transfer your cards to the new device in one easy step.” Moreover, many users opt to use iCloud backups to ensure an easy transition of data from one phone to another when upgrading to a new iPhone. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Backup allows users to create a backup of their device data, while iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple

devices. Thus, even if Hill switched iPhones since committing the crimes alleged in the criminal complaint, there is probable cause to believe the device still contains evidence of those crimes. Additionally, because Hill had multiple, prepaid debit cards and the Device on him when he was arrested, and because prepaid debit cards are commonly used to store, transfer, and conceal fraud proceeds, there is probable cause to believe that the Device contains evidence of more recent criminal conduct beyond that charged in the criminal complaint.

16. The Device is currently in storage at the HSI Portland, ME evidence room, located at 1 City Center, 4th Floor, Portland, ME 04103. In my training and experience, I know that the Device has been stored in a manner such that its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of HSI.

17. Based on the foregoing, I believe there is probable cause that the Device was an instrumentality of, and contains evidence of, federal crimes, including bank fraud, in violation of 18 U.S.C. § 1344, and aggravated identity theft, in violation of 18 U.S.C. § 1028A.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as

direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when.

There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- e. I know that when an individual uses an electronic device to gain unauthorized access to a victim’s electronic banking information, the individual’s electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of

the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.


20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

21. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

22. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



David Fife
HSI Special Agent

Sworn to telephonically and signed
electronically in accordance with the
requirements of Rule 4.1 of the Federal Rules
of Criminal Procedures

Date: Jul 09 2024

City and state: Portland, Maine



Judge's signature

Karen Frink Wolf, U.S. Magistrate Judge
Printed name and title